Roli i Forenzikës Kompjuterike në hetimin e rasteve me krime kibernetike

UBT, Prishtinë Kosovë

PERMBAJTJA

HYRJE

Në përdorimin e pajisjeve elektronike/digjitale, duhet të jemi të vetëdijshëm se ne jemi duke lënë një gjurmë pas vetes, një gjurmë digjitale. Të dhënat e telefonit mobil, transaksionet bankare, ueb shfletimet, e-mail-at, tekst mesazhet, fotografitë, audio-të, dhe video-të digjitale janë disa nga gjurmët që ne lëjmë pas. Gjurmët e tilla në forenzikën kompjuterike konsiderohen dhe quhen prova digjitale.

Forenzika Kompjuterike nuk mund të bëhet apo të hyjë në përdorim pa gjetur diçka të dyshimtë dhe të paligjshme apo pa i pasur duart e pista.
Rritja e internetit dhe përhapja e kompjuterëve në mbarë botën ka rritur nevojën për hetime kompjuterike.
Kompjuterët mund të përdoren për të kryer krime kibernetike dhe krimet mund të regjistrohen në kompjuter.
Gjithnjë e më shumë, pajisjet digjitale si kompjuterët, laptopët, telefonat e mençur, kamerat, etj., gjenden në skenat e krimit gjatë një hetimi penal.
Si përgjigje ndaj rritjes së krimit kibernetik, është shfaq fusha e Forenzikës Kompjuterike.

Forenzika Kompjuterike është përdorur dhe vazhdon të përdoret për të kryer hetime brenda kompjuterëve.

DEFINICIONI DHE RËNDËSIA E FORENZIKËS KOMPJUTERIKE

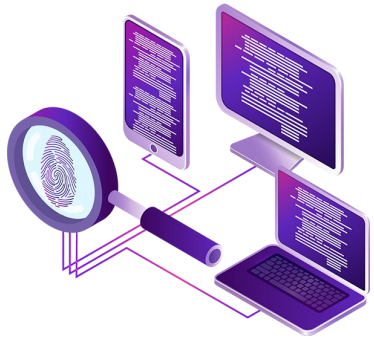
Çka është Forenzika Kompjuterike ?

- Është një proces special që përfshin analizën e Informacionit të Ruajtur Elektronik (IRE) që ruhet në pajisje elektronike, të tilla si kompjutera desktop, laptopë dhe disqe të jashtme të ngurta (ang. external hard drives).
- Është shkenca e gjetjes, ruajtjes, marrjes dhe paraqitjes të të dhënave që janë përpunuar në mënyrë elektronike dhe janë ruajtur në mediumet kompjuterike.

Forenzika Kompjuterike merret me kërkimin e kompjuterëve për provat e krimeve të kryera përmes përdorimit të kompjuterëve, të njohura si Krime Kibernetike.

Ajo gjithashtu merret me një bollëk informacioni, të dhënash dhe provash digjitale.

- Duke filluar nga log-at (historia e shfletimit në internet), deri tek fajll-at aktualë në disk.



Informacioni i mbledhur ndihmon në:

- arrestimin,
- ndjekjen penale,
- largimin nga puna, si dhe parandalimin e aktiviteteve të ardhshme ilegale të të dyshuarve.

Forenzika Kompjuterike mund të përmirësojë sigurinë e sistemit duke hetuar se si kryhen sulmet.

ROLI DHE OBJEKTIVAT E FORENZIKËS KOMPJUTERIKE

Forenzika Kompjuterike luan rol në:

- Identifikimin e krimit kibernetik
- Mbledhjen e provave digjitale
- Mbrojtjen e provave digjitale
- Analizimin e provave digjitale
- Paraqitjen apo prezantimin e provave digjitale
- Zbulimin e të dhënave në një sistem kompjuterik
- Ndjekjen penale

Objektivat kryesorë të forenzikës kompjuterike:

- Të rimarrë (rikthej), mbledhë, analizojë, dhe ruajë të dhënat kompjuterike dhe materialet përkatëse në një mënyrë që mund të paraqiten si provë në një gjykatë.
- Të identifikojë provat në një kohë të shkurtër, dhe të vlerësojë ndikimin e mundshëm të aktiviteteve dashakeqe mbi viktimën dhe të vlerësojë qëllimin dhe identitetin e kryerësit

RREGULLAT E FORENZIKËS KOMPJUTERIKE

Provat e mbledhura digjitale shpesh janë prova të vlefshme dhe si të tilla ato duhet të trajtohen në të njejtën mënyrë si provat tradicionale të forenzikës tradicionale, me respekt dhe kujdes.

Rregulli 1:
Një ekzaminim nuk duhet të kryhet në mediumin apo mjetin origjinal.
Rregulli 2:
Hetuesi duhet të bëjë kopje të provave origjinale dhe të fillojë ekzaminimin vetëm në kopje.
Rregulli 3:
Kopja duhet të jetë një replikim i saktë i origjinalit (d.m.th duhet të jetë identikë si origjinali, bit për bit), dhe eksperti në këtë rast hetuesi duhet gjithashtu të vërtetojë kopjen në mënyrë që pyetjet e ngritura kundër integritetit të provave të shmangen.
Rregulli 4:
Kompjuteri dhe të dhënat në të duhet të mbrohen gjatë përvetësimit (nxjerrjes) të mediumit apo mjetit për të siguruar që të dhënat nuk janë ndryshuar apo modifikuar.
Rregulli 5:
Duhet dokumentuar çdo ndryshim në prova.

METODOLOGJIA E FORENZIKËS KOMPJUTERIKE

Për shkak të keqpërdorimit në rritje të kompjuterëve në aktivitetet kriminale, duhet të ekzistojë një grup i duhur i metodologjive për t'u përdorur në një hetim.

***Ruajtja**:* Hetuesi i forenzikës kompjuterike duhet të ruajë integritetin e provave origjinale.
Provat origjinale nuk duhet të modifikohen ose dëmtohen. Hetuesi i forenzikës kompjuterike duhet të bëjë një *imazh* ose një kopje të provave origjinale dhe më pas të kryejë analizën në atë *imazh* ose kopje. Hetuesi gjithashtu duhet të krahasojë kopjen me provën origjinale për të identifikuar çdo modifikim ose dëmtim.

***Identifikimi**:* Para fillimit të hetimit, eksperti i forenzikës kompjuterike duhet të identifikojë provat dhe vendodhjen e tyre. Për shembull, provat mund të jenë të përfshira në HDD, USB, karta memorizuese, ose në llog fajlla.

***Nxjerrja**:* Pas identifikimit të provave, hetuesi i Forenzikës Kompjuterike duhet të nxjerrë të dhënat prej tyre. Meqenëse të dhënat e paqëndrueshme mund të humbasin në çdo pikë, hetuesi i forenzikës kompjuterike duhet t'i nxjerrë këto të dhëna nga kopja e bërë nga prova origjinale. Këto të dhëna të nxjerra duhet të krahasohen me provat origjinale dhe të analizohen.

METODOLOGJIA E FORENZIKËS KOMPJUTERIKE VAZHDIM (2)

Interpretimi: Roli më i rëndesishëm që një hetues i forenzikës kompjuterike luan gjatë hetimeve është të interpretojë (shpjegojë) atë që ai ose ajo ka gjetur në të vërtetë. Analiza dhe inspektimi i provave duhet të interpretohet në një mënyrë të qartë.

Dokumentimi: Nga fillimi i hetimit deri në fund (kur provat paraqiten para gjykatës), hetuesi i forenzikës kompjuterike mbanë dokumentacion në lidhje me provat. Dokumentacioni përfshin formularin e zingjirit të kujdestarisë dhe dokumentet në lidhje me analizën e provave.

Zingjir i kujdestarisë i referohet rendit në të cilin provat janë trajtuar gjatë hetimit të një çështjeje.

Është proces që ndjek/gjurmon lëvizjen e provave përmes dokumentimit të secilit person që ka trajtuar provat, datën/kohën kur janë mbledhur ose transferuar, dhe qëllimin e transferimit të provave.

HETUESIT E FORENZIKËS KOMPJUTERIKE

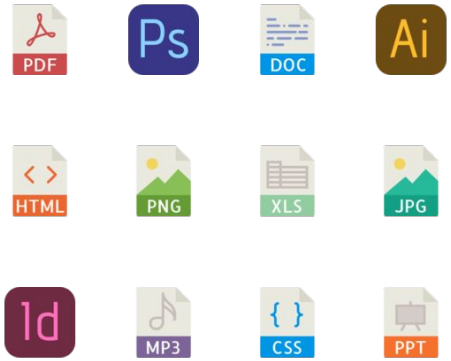
Personat që zbulojnë provat digjitale të veprimtarisë kriminale dhe ndihmojnë sjelljen e kryerësve të veprës penale para drejtësisë quhen specialistë, hetues, ose teknikë të Forenzikës Kompjuterike.

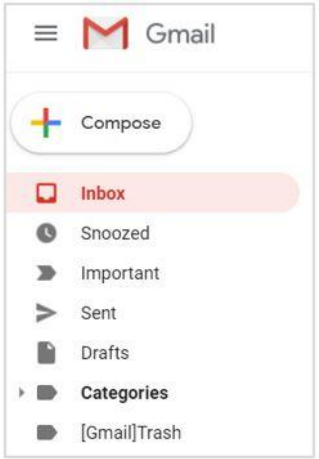
Një hetues i forenzikës kompjuterike kryen këto detyra:
- Përcakton shkallën e dëmit të shkaktuar gjatë krimit;
- Rikuperon (rikthen) të dhëna me vlerë hetimore nga kompjuterët e perfshirë në krime;
- Siguron që provat të mos dëmtohen në asnjë mënyrë;
- Krijon një imazh (kopje duplikate) të provës origjinale pa e manipuluar atë për të ruajtur integritetin e provës origjinale;
- Udhëzon zyrtarët në kryerjen e hetimeve;
- Rindërton disqet e dëmtuara ose pajisjet e tjera të ruajtjes dhe zbulon informacionin e fshehur në kompjuter;
- Analizon të dhënat e gjetura të provave;
- Përgatit raportin e analizës dhe bën dokumentimin e rastit;
- Adreson çështjen në një gjykatë dhe përpiqet të fitojë çështjen duke dëshmuar në gjykatë.

PROVAT DIGJITALE

Prova digjitale është çdo informacion i ruajtur në pajisje digjitale që mund të përdoret në gjykata.

Disa shembuj të llojeve të provave digjitale janë:
- Mesazhet elektronike (e-mail-at)
- Videot dhe audiot digjitale
- Imazhet/fotografitë digjitale
- Historitë e shfletuesve të internetit
- IP adresat
- Fajllat e sistemit dhe të programeve
- Fajllat e përkohshëm
- Të dhënat e ekstraktuara (nxjerra) nga pajisjet GPS dhe telefonat e mençur,etj..





Në përgjithësi, kriminelët shpesh lënë gjurmë (prova) digjitale në pajisjet e tyre digjitale.

PROVAT DIGJITALE (2) - VAZHDIM

Burimet e provave digjitale

Provat digjitale mund të gjenden në çdo medium digjital, duke përfshirë këtu:

- *Kartat memorizuese, USB-të pajisjet e lëvizshme (Removable Media):*

  - Pavarësisht nga madhësia e tyre e vogël, kartat memorizuese mund të mbajnë mijëra prova të mundshme si p.sh: pornografia e fëmijëve, numrat e vjedhur të kredit kartelave, fotografi, video, fajlla, vegla për hacking etj.

- *Pajisjet mobile*

  - Pothuajse të gjithë kemi një pajisje mobile në ditët e sotme. Ato shpesh përmbajnë disa prova shumë të vlefshme si p.sh: tekst mesazhe, e-mail mesazhe, regjistra të thirrjeve(logs), gjeo-lokacionin, kontakte, etj.

- *Kompjuterët, laptopët, pajisje të rrjetës, pajisje periferike(CD,DVD,kamera digjitale,HDD external,etj), mjedise "cloud".*

PROVAT DIGJITALE (3) - VAZHDIM

Burimet e provave digjitale

MBLEDHJA E TË DHËNAVE (PROVAVE) DIGJITALE

Hapi i parë në çdo ekzaminim të forenzikës kompjuterike është mbledhja e provave.
Gjatë mbledhjes së provave, renditja e mbledhjes duhet të vazhdojë nga provat më të paqëndrueshme deri tek provat më të qëndrueshme.

Procesi i mbledhjes së provave në terma të përgjithshëm mund të ndahet në njërën nga dy kategoritë.
Këto dy kategori njihen edhe si:

1. *sistem i drejtëpërdrejtë* – kur kompjuteri është i ndezur (ang. live system)
    - Përmbajtja e RAM-it mund të përmbajë informacion jetësor. I gjithë ky informacion jetik do të humbasë kur kompjuteri fiket/mbyllet ose kur hiqet furnizimi me energji elektrike. Qëllimi i një hetimi të drejtëpërdrejtë është të mbledh dhe të ruajë sa më shumë të dhëna të paqëndrueshme që janë aktive në momentin që është i ndezur kompjuteri në mënyrë që këto të dhëna mos të humbasin.
2. *sistem i vdekur – kur kompjuteri është i fikur* (ang. dead system)
    - Këtu ekzistojnë vetëm të dhënat e ruajtura në memorien statike, siç është një disk i ngurtë ose USB, që duhet të ekzaminohen. Të dhënat nuk humbasin kur kompjuteri fiket dhe hiqet burimi i energjisë të sistemit.

ANALZIMI I TË DHËNAVE (PROVAVE) DIGJITALE

Analizat duhet të kryhen në kopje të provave në mënyrë që të shmanget çdo modifikim, duke ruajtur vlefshmërinë dhe besueshmërinë e të dhënave.
Duke analizuar provat e marra gjatë hetimit të forenzikës së kompjuterit, hetuesit përpiqen të kuptojnë se çfarë ka ndodhur, kur ka ndodhur, si ka ndodhur, pse ka ndodhur dhe kush ishte i përfshirë.
Procesi i analizimit të imazheve (të kopjes të të dhënave) varet shumë nga natyra e dyshuar e incidentit.

- P.sh: personat (kriminelët/të dyshuarit) me më shumë njohuri teknike potencialisht kanë aftësinë për të fshehur të dhënat brenda sistemit në mënyrë më efektive, prandaj këto raste kërkojnë një qasje dhe nivel tjetër të analizës.

Sa i përket analizimit të diskut të ngurtë, ashtu sikurse mbledhja e të dhënave ajo mund të arrihet në dy mënyra:

1. analiza e drejtëpërdrejtë (ang. live analysis)
2. analiza e vdekur (ang. dead analisys)

Tradicionalisht, procedura e forenzikës kompjuterike është përqendruar në analizën e vdekur – kur kompjuteri/sistemi është i fikur.
Kjo mënyrë përdoret më shpesh pasiqë të dhënat në *imazh* nuk ndryshojnë kurrë dhe integriteti i të dhënave është më i thjeshtë për t'u ruajtur.
Për shumicën e hetimeve, kjo formë e analizës është e mjaftueshme.

KATEGORITE E TË DHËNAVE (PROVAVE) DIGJITALE

Gjatë hetimit të një rasti kriminal kompjuterik hetuesit mund të hasin tri kategori apo tri tipe të të dhënave.

1. Të dhënat aktive

- Janë të dhënat që ne përdorim çdo ditë në kompjuterin tonë. Hetuesit mund t'i gjejnë këta fajlla duke përdorur *Windows Explorer*. Këta janë fajllat që qëndrojnë në hapësirën e caktuar (ang. allocated) të diskut.

Të dhënat aktive janë: fajllat e ndryshëm, programet dhe të dhënat që janë në përdorim nga sistemi operativ, të tilla si: dokumentet, fotografitë, e-mail-at, dritaret e shfletuesve të internetit, etj.

2. Të dhënat e fshehura

- Të dhënat që ekzistojnë pavarësisht së janë fshirë apo ri-emëruar. Këto të dhëna nuk janë më të gjurmuara nga Sistemi Operativ dhe për këtë arsye janë të "fshehura/të padukshme" për përdoruesin mesatar. Mund gjenden në hapësirën e pa alokuar (ang. unallocated space). Për kthimin e të dhënave të tilla kërkohet përdorim i veglave dhe teknikave të specializuara. Të dhënat e fshehura janë të shtrenjta dhe marrin kohë deri në zbulimin e tyre.

3. Të dhënat e arkivuara

Të dhënat në backup. Mund të ruhen në CD, USB, HDD, SD karta, dhe në "cloud".

KATEGORITE E TË DHËNAVE (PROVAVE) DIGJITALE VAZHDIM (2)

Gjithashtu gjatë hetimit mund të hasim në dy lloje të informaionit:

1. Informacionet e paqëndrueshme

● Gjenden kryesisht në RAM-in kryesor të kompjuterit. RAM-i zakonisht përdoret për të ruajtur përkohësisht të dhënat e ekzekutuara të programit.
Këto të dhëna humbasin kur hiqet burimi i energjisë.

Llojet e të dhënave që gjenden në RAM përfshijnë:
- Proceset aktive (Programet, shërbimet dhe sesionet aktualisht të ngritura në sistem)
- Përdoruesit e kyçur (Përdoruesit apo punonjësit që janë duke e përdorur aktualisht sistemin)
- Fjalëkalimet me tekst të pastër
- Të dhënat të pakriptuara

2. Informacionet e qëndrueshme

● Gjenden kryesisht në të gjitha llojet e mediumeve të tjera që nuk humbasin të dhënat e tyre kur kompjuteri fiket dhe hiqet burimi i energjisë të sistemit.

Disa nga mediumet me memorie të qëndrueshme janë:
● HDD-të
● USB-të
● iPod-at
● SD karta-at

VEGLAT E FORENZIKËS KOMPJUTERIKE

Veglat e forenzikës kompjuterike e bëjnë punën e hetuesve shumë më efikase.
Veglat e Forenzikës Kompjuterike mundësojnë që hetuesi i Forenzikës Kompjuterike të rikuperojë (rikthej) fajllat e fshirë, fajllat e fshehur, dhe të dhënat e përkohshme që përdoruesi (i dyshuari) mund të mos i lokalizojë.

Ka vegla për qëllime specifike, si dhe vegla me funksionalitet më të gjerë.
Ato mund të ndahen në dy forma apo në dy kategori:

- Vegla harduerike të Forenzikës Kompjuterike
- Vegla softuerike të Forenzikës Kompjuterike

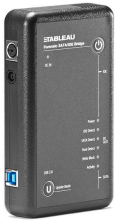
Gjithashtu, ato mund të jenë:

- Vegla komerciale që duhet të blihen
- Vegla me burim të hapur (ang. open source) që janë në dispozicion pa pagesë (falas).

VEGLAT E FORENZIKËS KOMPJUTERIKE
VEGLAT HARDUERIKE

Veglat harduerike të Forenzikës Kompjuterike variojnë nga ato të thjeshtat deri tek ato më të komplikuarat.
Disa nga këto vegla përfshijnë:

- Pajisje per ruajtjen, dyfishimin, verifikimin, kthimin, analizimin e të dhënave (provave) digjitale;
- Pajisjet ruajtëse portative;
- Bllokues shkrimesh, p.sh Tableau T35U, Wiebitech Forensic UltraDock v5;
- Adaptorë;
- Kabllo;
- Kuti veglash (stilolapsa, kamera digjitale, mediume të pastra për ruajtje, çanta provash, formularë raporti, dorëza, dhe të ngjashëm).



VEGLAT E FORENZIKËS KOMPJUTERIKE
VEGLAT SOFTUERIKE

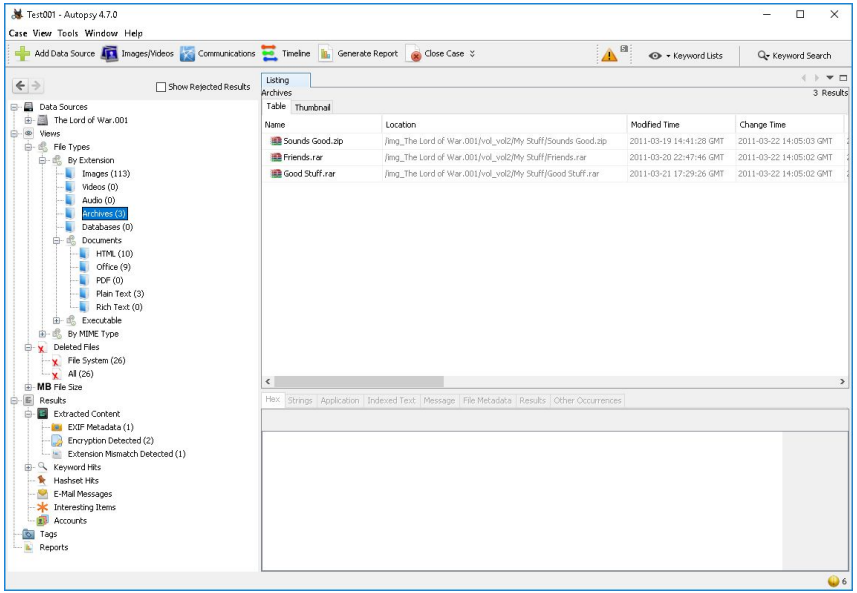
Veglat softuerike të Forenzikës Kompjuterike grupohen në:

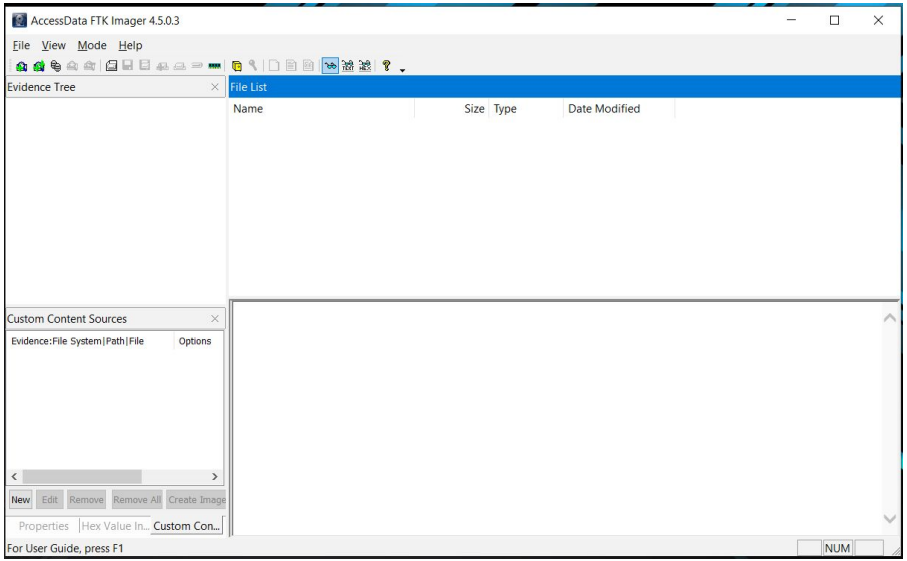
- CLI aplikacione
- GUI aplikacione

Po ashtu veglat softuerike mund të ndahen në:

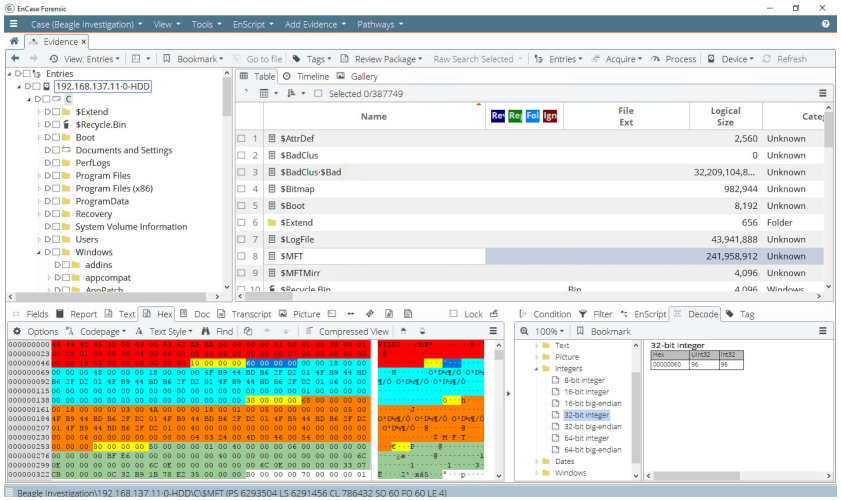
- Me burim te hapur (pa pagesë):
  1. Autopsy
  2. Photorec
  3. Eric Zimmerman Tools
  4. SIFT Workstation
  5. FTK Imager
- Me pagesë (komerciale):
  1. FTK (Forensic Toolkit, AccessData)
  2. EnCase (Guidance Software)
  3. ProDiscover
  4. OSForensics
  5. X-Ways
  6. Helix3 Pro

VEGLAT E FORENZIKËS KOMPJUTERIKE
VEGLAT SOFTUERIKE (2) - VAZHDIM





VEGLAT E FORENZIKËS KOMPJUTERIKE
VEGLAT SOFTUERIKE (3) - VAZHDIM



Faleminderit!

UBT, Prishtinë, Kosovë